PROTECTING THE HOMELAND

In the wake of the September 11 attacks, our government acted with unprecedented unity and speed. The Administration was authorized to take a variety of actions to protect us from terrorists, including the use of military force against al-Qaeda and the Taliban. In the months following September 11, legislation was enacted to bolster security at our seaports and airports, fortify our borders, and provide our intelligence and law enforcement communities with the tools needed to root out terrorists here and abroad. The following year we worked together to create the Department of Homeland Security.

These efforts, the implementation of many new programs, and increased funding for many established programs, have made us safer today than we were before the attacks of September 11. But the critical question is – are we as safe as we need to be?

It remains an uncomfortable but unassailable fact: America is not as safe as it needs to be in the face of the threat we face from those that seek to do us harm. Critical gaps in our homeland security continue to exist while, as the Madrid train bombing confirms, al-Qaeda and like-minded groups continue to seek ways to kill our citizens, destroy property and infrastructure, disrupt our economy, and demoralize our nation. Our enemies are opportunistic and will remain fixated on identifying and exploiting our weaknesses. We must be proactive in taking steps to prevent attacks in America and remain vigilant in bolstering our homeland defenses as rapidly and effectively as we can. As we move forward to strengthen our security we must be mindful that properly made, homeland security-related investments also offer substantial benefits in such critical areas as public health, crime prevention, technology development, the free flow of commerce, and all-hazards preparedness.

We also need to acknowledge the somewhat counterintuitive reality that our homeland security efforts start on foreign shores. The greatest threat to our security and the future of the globe, is the possibility that terrorist groups obtain and use a nuclear weapon. One of the fundamental measures we must take to protect our homeland is to secure stockpiles of nuclear materials around the globe, as well as other materials that could be used to develop weapons of mass destruction. We must also take aggressive measures to deal with the threat of bioterrorism, ranging from developing the capacity to develop countermeasures to bioengineered pathogens to planning mass vaccination campaigns in the event of an attack.

Stronger measures also need to be taken to protect our borders and harden targets inside America. The entry of 20 million cargo containers into America by ship, rail, and truck presents a tremendous vulnerability and our efforts to close this security gap have thus far been inadequate. And we still do not have in place effective measures to screen foreign visitors coming to the United States and reduce the flow of illegal immigration as well. While massive investments have been made in aviation, unscreened air cargo and shoulder fired missiles present serious threats to security. Inside

the United States, little has been done since September 11 to better secure our food supply, our computer networks, our rail and transit systems, and other critical infrastructures.

If our defenses fail, our first responders need to be better prepared than they are now to deal with the consequences of a terrorist attack. Homeland security spending can no longer be treated as another source of port barrel spending – we must target funds where they are needed most and ensure they are dedicated toward building the essential capabilities of our first responder communities to respond to terrorist attacks. At a minimum, strong federal efforts need to be taken to solve the communications interoperability problem that tragically plagued the response efforts at the World Trade Center.

Providing for the common defense is the first duty of government. To win the war on terror, we must dedicate ourselves to making the changes necessary and committing sufficient resources to protecting the country against the serious threats we still face every day.

PREVENTING TERRORISTS FROM OBTAINING WEAPONS OF MASS DESTRUCTION

The chilling reality is that terrorists have been working for a decade to acquire weapons of mass destruction. Indeed, DCI George Tenet recently testified that "acquiring these [weapons] remains a religious obligation in Bin Ladin's eyes."[44] Yet, tons of WMD material is strewn across the globe at insecure locations, ripe for their picking. The International Atomic Energy Agency reports that there have already been 16 thefts involving highly enriched uranium (HEU) and plutonium.[45] In one case, the theft of about two kilograms of HEU from a research facility in the nation of Georgia, the whereabouts of the material remain unknown.[46]

We can take important steps toward preventing terrorist's acquisition of weapons of mass destruction if we take bold and decisive action and build a global coalition to halt the spread of WMD.

Unfortunately, this critical mission is not being accomplished. For example, the United States has increased spending for programs focused on improving controls over nuclear and chemical warheads, materials, and expertise outside the U.S. by only 8% since September 11, 2001.[47] We must act with the speed and commitment of a nation trying to protect our people from the horrific fate of nuclear devastation or the plagues that could be unleashed from bio-terrorism.

In the words of former U.S. Senator Sam Nunn, "Terrorist groups are racing to get weapons of mass destruction. We should be racing to stop them." [48]

Secure All Unprotected Nuclear Material

Ten years ago, the Soviet Union broke apart and left as its legacy enough highly enriched uranium and plutonium to make 60,000 nuclear warheads. Much of this material is unguarded and unaccounted for.[49] The largest stock of unsecured nuclear material is in Russia and some of its former Republics. This threat, however, extends far beyond Russia and the former Soviet Union. Some twenty tons of highly enriched uranium (HEU) exist at 130 civilian research facilities in 40 countries, many of which have no more security than a night watchman and a chain link fence.[50] Furthermore, we haven't fully accounted for sealed sources of nuclear material on loan to foreign countries. [51] The solution to the problem is clear, as Senator Nunn stated, "The most effective, least expensive way to prevent nuclear terrorism is to secure weapons and materials at the source.[52] If terrorists could get hold of the HEU or plutonium that are essential ingredients of a nuclear bomb, making a bomb might be within the capabilities of al-Qaeda.[53]

While the United States and Russia have been working together to secure these materials in Russia for over ten years, to date even initial "rapid upgrades" such a bricking over windows or piling heavy blocks on top of material, have been accomplished for only 40% of the potential bomb material in Russia. Less than one-seventh of Russia's stockpile of highly enriched uranium has been destroyed.[54]

In June 2002, the leaders of the Group of Eight (G-8) industrialized democracies agreed to launch a new "Global Partnership Against the Spread of Weapons of Mass Destruction." The purpose of the Global Partnership is "to prevent terrorists, or those that harbor them, from acquiring, or developing, nuclear, chemical, biological, missile, and related technology." The G-8

committed $20 billion over the next ten years to threat reduction projects.[55] Unfortunately, many Nunn-Lugar programs are on hold because of access and liability issues that have been problems for years. Russia is denying the U.S. access to the most significant sites that need robust security, and we have not resolved the Russian concerns about the liability requirements for U.S. contract personnel performing the security upgrades.

It is time for the United States to lead the Global Partnership toward decisive action aimed at preventing nuclear terrorism with initiatives such as:

Secure Nuclear Material Across the Globe

During the Cold War, the United States and Russia built dozens of nuclear energy research labs in other nations across the globe. Twenty tons of HEU were distributed around the world in the last fifty years by the U.S. and the Soviet Union into research reactors and other facilities.[56] Most of this material is poorly guarded.

> *The United States should lead an effort through the International Atomic Energy Agency, to secure all nuclear material locations outside the U.S. and Russia in the next two years. Armed guards, electronic surveillance, and layered barriers and defenses would be employed.*

Remove All Nuclear Material from the World's Most Vulnerable Sites

The surest way to ensure that nuclear material will not be stolen from one of the 130 vulnerable sites around the world is to remove it so there is nothing left to steal. A successful joint U.S.-Russian operation did precisely this at the Vinca reactor in Belgrade, Serbia just last year. One hundred pounds of highly vulnerable nuclear fuel was removed and secured.

> *The United States should lead an effort with our G-8 partners to remove all nuclear material from vulnerable sites outside Russia within the next five years. Such an effort could be accomplished for under $50 million a year.*[57]

Secure Nuclear Materials From Russia and the Former Soviet Union by 2008

Hundreds of tons of weapons grade nuclear material in Russia remains at locations that are not secure and are vulnerable to theft and terrorist attack.

> *The United States, along with its Global Partners, should secure all weapons grade nuclear material in Russia and the states of the former Soviet Union within the next five years. This requires a committed, aggressive effort to eliminate the access and liability barriers to securing this material.*

Triple U.S. Commitment to Nuclear Security

Funding for the Cooperative Threat Reduction Programs "Nunn-Lugar" has remained flat over the last several years at about $1 billion annually. A bipartisan Commission under Howard Baker and Lloyd Cutler proposed last year that U.S. efforts for nuclear security be increased to $30 billion over ten years.[58]

The United States should meet the goals of the Baker-Cutler Commission and triple the resources spent to improve nuclear security.

Strengthen Counterproliferation Efforts

The unraveling of Pakistani scientist A.Q. Khan's nuclear smuggling network has revealed that the spread of nuclear weapons expertise and development equipment is a problem of global proportions. The absence of an international legal regime to constrain such activities badly complicates efforts to penalize proliferators such as A.Q. Khan and his partners. Under an international legal regime requiring transparency, Khan's network and recipient states would have put themselves in jeopardy of capture and prosecution by any state in the world when they failed to disclose their activities. To deter, protect against, and punish proliferators, the United States must work with the rest of the international community to develop laws with universal jurisdiction that enable enforcers to reach anywhere that dangers arise.

Criminalize Nuclear Smuggling

The United States should take the lead in proposing a new international convention that will facilitate the detection, interdiction, and enforcement against individuals, corporations and states that might engage in illicit acquisition, possession, development, and trafficking of nuclear weapons related materials, equipment, and know-how. Such a Convention would criminalize transfer or trade in nuclear weapons components and require a declaration system for legitimate trade across state borders while rendering undeclared trade illegal.

Develop an International Strike Force to Hunt Nuclear Traffickers

Currently the IAEA has three full time personnel who work on preventing illicit trafficking in nuclear material.

The United States should support the creation of a 50 person international law enforcement unit to track nuclear smugglers.

Expand Proliferation Security Initiative

In the spring of 2003 the Bush Administration brought together a coalition of ten other nations who were willing to "enter into partnerships to employ their national capabilities to develop a broad range of legal, diplomatic, economic, military and other tools to interdict threatening shipments of WMD and missile related technology."[59] The PSI envisions being able, if necessary, to interdict WMD transfers on the high seas or in the territory of partner states. Though PSI has expanded to include additional supporters, to date, China and Russia have refused to participate in this initiative citing a number of concerns related to the legality of interdiction. Russian and Chinese participation is important to the success of this initiative.

The 26 nations of the North Atlantic Treaty Organization have a long established network of intelligence sharing, shared military practices built through exercises, interoperable equipment and joint planning structures. PSI can be made operationally more effective by using the existing structure of NATO.

> *The United States should encourage every NATO state to sign on to the Proliferation Security Initiative and use NATO's training, exercise and planning structure to enhance PSI's operational capability. Further, PSI membership should be open to non-NATO countries and China and Russia should be encouraged to participate.*

Secure Sources For "Dirty Bomb" Materials

Al-Qaeda has expressed interest in unleashing radiological terrorism by building and using radiological dispersal devices (RDDs) that are also known as "dirty bombs." In April, 2002, a captured Al-Qaeda leader, Abu Zubaydah, told American interrogators that the organization had been working aggressively to build a so-called "dirty bomb."[60] In February 2004, George Tenet, the CIA Director, stated that Al-Qaeda remains interested in dirty bombs and terrorist documents contain accurate views of how such weapons would be used.[61]

Common radioactive materials that are used in medicine, industry and scientific research, could fuel RDDs.[62] Though only a small fraction of the millions of radioactive sources used worldwide pose inherently high security risks, this category in absolute numbers encompasses hundreds of thousands of sources all over the word.[63] With so many potential sources, we should focus our defensive measures on those elements that are most hazardous, such as strontium, cesium, and plutonium. Important next steps include:

Strengthen Domestic Inspection

> *The Nuclear Regulatory Commission should increase the inspections of users of the most radioactive materials.*

Secure Disused Sources

The Department of Energy's Off-Site Recovery Project has secured more than three thousand disused sources of radioactivity, but faces substantial funding shortfalls.[64]

> *The Department of Energy should secure ten thousand disused radioactive sources of cesium, strontium and plutonium in the next two years.*

Encourage International Action

Dozens of nations across the globe are home to thousands of pounds of source material for potential use in radiological devices. The United States should help lead an international effort to identify and secure these source materials.

The United States should strengthen the International Atomic Energy Agency to offer regulatory and security assistance to the 50 non-members states that lack security and regulatory infrastructure for radioactive sources.[65]

Destroy Chemical Weapons Stockpiles

The deadly effects of chemical weapons have been known since the First World War. We were reminded of their horrible capability during the Iran-Iraq war and after learning of how Saddam Hussein in Iraq used them to exterminate whole villages of civilians.

Today, chemical weapons are of particular interest to international terrorists as a poor man's weapon of mass destruction. Terrorists have used chemical weapons in the subways of Tokyo, and toxins have been used in suicide bombings in Israel and have been tested by al-Qaeda terrorists working in Afghanistan.[66]

At the Shchuchye chemical weapons facility in Russia, there are today nearly 2 million rounds of nerve agents – enough to kill every man, woman, and child on earth. One artillery shell is small enough to fit in a briefcase and kill one hundred thousand people.[67] The weapons sit in decaying buildings, largely unsupervised. The threat of unsecured chemical weapons falling into the hands of terrorist is a real threat and wholly preventable.

The United States and Russia have agreed to destroy their stockpiles of chemical weapons, which account for 90% of existing global stockpiles.[68] Yet, most of Russia's 40,000 tons of chemical weapons … have yet to be destroyed.[69] In 1998, the United States Senate ratified the Chemical Weapons Convention (CWC), which bans the development, production, stockpiling, and use of chemical weapons, requires the destruction of existing weapons and related material, establishes an international verification regime, and requires export controls and punishment for violators of the Convention.[70]

Current law calls for the destruction of chemical weapons by 2012, but the United States has a poor record of destroying its own stockpile. According to the Department of Defense, management, organizational, and strategic planning weaknesses are causing the U.S. to miss the CWC's 2004 deadline for eliminating 45 percent of our chemical stockpile. Addressing its own program will help the U.S. make the case that other countries should follow its lead.

The United States should lead by example by improving its efforts to eliminate its own chemical weapons stockpiles on time. It should also promote an international effort to destroy all chemical weapons worldwide in the next six years. The U.S. should offer all technical and financial assistance necessary to locate, secure and destroy stockpiles of chemical weapons globally. As part of this assistance package, nations receiving aid will be asked to support a sanctions regime against any and all nations refusing to join the Chemical Weapons Convention.

PROTECTING AGAINST THE THREAT OF BIOTERRORISM

Biological weapons are one of the most frightening of all weapons of mass destruction and are a growing threat. History shows us the threat of contagion is real. In the 20th century alone, more than 300 million people died from smallpox.[71] Today, infectious diseases remain the third leading cause of death in the U.S.[72] The anthrax attacks of October-November 2001 demonstrated that the capability and the will to murder with pathogens are now a reality.

Compared to nuclear or chemical weapons, weapons for bioterrorism are easy to obtain and produce, inexpensive, and capable of inflicting significant damage even in the absence of large quantities of material or delivery mechanisms.[73] Pathogens suitable for attacks can be concealed and transported with little difficulty. Information about how to obtain and prepare dangerous pathogens is increasingly available through the Internet and other open sources. Furthermore, bioweapons facilities can be easily concealed within legitimate research laboratories or pharmaceutical sites.[74]

During the Second World War, it was learned that Nazi Germany was attempting to develop a super weapon that could inflict millions of casualties and lead to our defeat. In response, the United States mobilized the federal government on a massive scale and the "Manhattan Project" produced the atomic bomb first and helped to win the war. The threat of bioterrorism to our national security is so great that the United States should embark on a "Bioterrorism Prevention Initiative" of such scale and ambition that it will rival the Manhattan Project. Such an initiative would be comprised of the following elements:

Prevent Terrorists From Obtaining Biological Weapons

The dangerous legacy of the massive Soviet biological weapons program remains at dozens of former research and production sites across former Soviet states.[75] Planning, funding, and diplomatic pressure to secure and track activities at these locations has languished. Currently there are 140 nations that have ratified the Biological Weapons Convention of 1972 that prohibits the possession, stockpiling and use of biological weapons. But the Convention, violated by the Soviet Union during the Cold War, has never had provisions for monitoring, inspection, and enforcement.[76] Meanwhile, a thriving "germ commerce," including the exchange and storage of dangerous pathogens, continues throughout the world, with too few effective controls.[77]

> *The United States must lead an effort to put enforcement provisions in the Biological Weapons Convention and develop international controls on pathogen research and trade. Technology to help detect and prevent weaponization should be developed and distributed to support enforcement. The U.S. should work with nations who agree to these enhanced protections to provide comprehensive vaccine stockpiles for their populations and improve their infectious disease surveillance capacity. The United States should work to strengthen the Cooperative Threat Reduction Program to secure foreign stockpiles of bioweapons, and champion standardized, international controls on the storage, sale and transport of dangerous pathogens.*

Protect Against Bioterrorism By Developing New Cures and Technologies

"Manhattan Project" for New Cures

Even with effective preparedness, we lack most of the diagnostics, drugs, and vaccines we would need to find those exposed, treat potentially life-threatening infection, and prevent disease from spreading. According to a 2000 study by the Defense Science Board, we have only one of the 57 different countermeasures needed to defend against 19 of the major bioterrorist agents.[78] Currently, the government lacks the capability to develop new medicines, while the private sector has little incentive to enter the biodefense market.[79] Project Bioshield, the Administration's attempt to solve this dilemma, does not go far enough in harnessing private sector capabilities or enhancing the federal capability to develop essential medical tools. An effective government effort to produce new medicines may finally address many of the serious national and international health problems that are neglected by traditional market forces and private pharmaceutical firms.

The United States should harness the innovation of the private sector and the power of the federal government in an effort akin to the "Manhattan Project" to develop effective treatments for the most dangerous diseases in the world. The federal government should develop the capacity to produce new, safe, and effective diagnostics, vaccines, and drugs against the most virulent pathogens to protect our citizens against bioterrorism and other serious infectious disease threats. Federally-funded venture capital and "virtual" drug development firms should be established to develop and utilize the best public, private, and academic scientific and technological capabilities to counter microbial threats.

Creating Rapid "Bug to Drug" Capability

The advancement of biotechnology is making possible the bioengineering of new weapons that can evade current detection and treatment strategies.[80] The emergence of SARS and novel virulent flu strains demonstrate how rapidly pathogens can naturally mutate to subvert our medical defenses. The danger of a thinking enemy manipulating pathogens in a similar way could be devastating. Under such circumstances we would have few options but to try to find existing or new medicines effective against the new disease. However, our response capabilities today are remarkably slow. Currently, it usually takes over ten years to develop a treatment for a new infectious disease.[81] However, the Defense Science Board has suggested that a sustained research effort over 20 years could reduce the time from pathogen identification to effective countermeasure, or "bug to drug," from ten years to 24 hours.[82] Opportunities here are rich. In a recent report, the Food and Drug Administration stated that technology in drug and vaccine development has long been neglected, noting that "in many cases, developers have no choice but to use the tools and concepts of the last century to assess this century's candidates."[83] The agency suggested a new research agenda is required to "turn the process of bringing these technologies to patients from a costly and time-consuming art form to a well-understood science" in order to cut drug and vaccine timeframes and costs. This research agenda could be the foundation of a strong public-private partnership effort to fight novel or bioengineered infectious diseases with the rapid delivery of drug and vaccine countermeasures.

The U.S. should embark on a long term research program aimed at dramatically shortening the time between the detection and identification of a new pathogen and the production of effective countermeasures to protect health. The "bug to drug" cycle should be shortened from years to a matter of weeks. The resulting

advances should be applied to a working capability to deliver cures to a novel or bioengineered pathogen as quickly as possible. Notably, the fruits of such an endeavor could provide many important benefits in addition to strengthening our biodefenses, including reduced drug costs and faster delivery of new medicines for all types of illnesses.

Prepare for Bioterror Attack by Building a Strong Biodefense System

Even with the strongest prevention efforts, the risk of terrorists deploying bioweapons cannot be completely eliminated. A strong biodefense system must be developed that prepares America for a bioterror attack and demonstrates to our enemies our ability to protect ourselves. Governments, first responders, and the healthcare sector must be given clear roles and responsibilities, and furnished with the capabilities to detect pathogens in the environment, identify exposed victims, and treat these individuals.

Develop a National Biodefense Plan

While one of the greatest threats to our health and safety remains the potential of a terror attack with biological agents, no comprehensive national plan has been developed to prevent, prepare for and respond to a bioterror attack.

A comprehensive National Biodefense Plan should be developed and implemented that defines roles and responsibilities for relevant federal, state, local, and private institutions and identifies and provides crucial capabilities required for effective preparedness.

Establish an Early Warning System

A National Health Tracking Initiative should be launched that establishes regional and national centers for the integration of laboratory, clinical, pharmacy, and other data relevant to monitoring population health. Connected to the Centers for Disease Control's Health Alert Network, these centers would provide an early-warning system for signs of infectious disease outbreaks.

Promote International Disease Surveillance

AIDS, SARS, and the West Nile virus demonstrate that pathogens can cross oceans and do not respect borders. Today, the world's cities are all reachable within 36 hours by air. A bioterror attack or naturally occurring outbreaks in other countries can spread quickly, making the ability to detect these incidents before they reach the U.S. a crucial defense.

The U.S. should lead international cooperative efforts in infectious disease surveillance, detection, and containment. The United States should also work through the World Health Organization to support units that can deploy any-

where in the world within 24 hours for emergency response to infectious diseases.

Build Public Health "Surge Capacity"

America's health care system and public health infrastructure are already stretched to capacity and would be unable to effectively respond to, or care for the mass casualties that could be expected from, a biological or other WMD attack on American soil.[84] While more attention and resources have been belatedly given to our health infrastructure since September 11, the system remains underprepared, with insufficient workers to distribute medicines, lack of hospital and laboratory surge capacity, and a chronic gaps in planning.[85] Disease surveillance, the essential first step in detecting an outbreak, is hampered by too few epidemiologists in the field and incomplete collection and integration of available health information at the regional and national level.[86] Stronger, better targeted, and sustained investment in our public health capacities is clearly necessary. Ultimately, a strong biodefense through public health preparedness will not only serve to deter a potential adversary from using biological weapons, but also prove invaluable for dealing with naturally occurring disease outbreaks, and many other public health concerns.

Strengthening the public health infrastructure must be a primary focus of our biodefense strategy and the National Biodefense Plan should help define where to target significantly increased and sustained new investments. Every hospital in the United States should receive the specialized tools necessary to diagnose and respond to biological attacks. Regional planning efforts for surge capacity should be initiated. Additionally, the federal government should consider mothballing Veterans Administration hospitals that are scheduled for closure and prepare them for use as mass casualty facilities during an emergency.

PROTECTING OUR BORDERS AND PORTS OF ENTRY

Our borders and ports of entry are one of the last lines of defense protecting the American people. It is essential that we dedicate the resources necessary to strengthen our defenses on land, sea, and air. While doing so, we must ensure that America remains a welcoming nation to visitors, students, and commerce. To both secure our borders, and ensure that they facilitate, rather than hinder, travel and trade, we must make investments in technology, personnel, and technology to modernize our borders and the surrounding communities for the 21st century.

Strengthen Land Borders

Increase Patrols and Inspectors on Our Borders

The United States must meet the need to screen cargo and visitors at the border and control the spaces between our ports of entry, while maintaining a free flow of commerce and an open door to visitors. Over 2000 new inspectors must be hired along the northern border just to meet the mandates set forth in the USA Patriot Act. The federal government has not even developed a new staffing strategy to deal with the security and immigration control issues on the southern border. Massive illegal immigration problems along the Arizona border have required the launching of a new federal initiative, but it is being staffed by transferring agents from other southern border sites. Genuine border security cannot be achieved by plugging one hole only to open up another.

The United States should increase the number of border inspectors and border patrol agents by at least 3,000 over the next four years. Staff should be allocated based on a national threat and vulnerability assessment to prioritize the threats facing our land borders and areas between our ports of entry.

Monitor Every Mile of the Border 24/7

Hundreds of miles of our border go unmonitored by personnel or technology every day. Yet technology currently exists – such as unmanned aerial vehicles, remote sensors, and long range cameras – to monitor every mile of the northern and southern border for the passage of terrorists and illicit cargo. [87]

The Department of Homeland Security must deploy innovative technologies to ensure that every mile of our land border is monitored.

Develop a Border Management System that Enhances Homeland Security and Facilitates Legitimate Travel and Trade

The US-VISIT entry-exit system proposes to improve border integrity by recording the entry and exit of foreign visitors to the United States and validating their identities. The program, which has been partially implemented at our air and sea ports, is in its infancy.

Full implementation of US-VISIT will prove immensely challenging, especially if current inadequacies in infrastructure, personnel, and technology are not addressed. Sixty-four land ports of entry have less than 25 percent of the required space in the federal inspections area.[88] Public highways and roads leading to ports of entry on both sides of the northern and southern border are insufficient.[89] Insufficient staffing at and between land border ports of entry, airports, and seaports has been an ongoing problem.[90] Enhancements in technology, without commensurate improvements in infrastructure and staffing may actually reduce the effectiveness of border security programs and substantially increase wait times at our borders. It is critical to understand that technology is an aid, not a replacement, for law enforcement personnel at our borders. Prior to full implementation of US-VISIT, the Administration must lay a solid foundation to create a vibrant and secure border through investments in infrastructure that will enable security to be enhanced while expanding economic opportunities and growth.

As an anti-terrorism tool, US-VISIT has potential, but must address glaring deficiencies. To be effective, the system must be capable of electronically screening individuals against a comprehensive integrated terrorist watch list. Right now, it cannot. Additionally, security could be enhanced by screening and inspecting as many foreign visitors as possible before they arrive in the United States. Lastly, while the security US-VISIT offers is limited to our ports of entry, border regions between ports of entry remain extremely porous.

The Administration should invest in adequate highways and access roads to the border, expanded inspection areas where possible, and additional inspections personnel and technology. The Administration should also move quickly to push out our border through the expansion of pre-clearance programs at our land borders and at our airports overseas. Lastly, the thousands of miles between our ports remain vulnerable unless we make necessary investments in law enforcement personnel and technology.

Protect Seaports

Strengthen the Coast Guard

Since September 11th, the U.S. Coast Guard has been asked to lead the nation's efforts to secure 95,000 miles of coastline and 361 ports while ensuring the flow of commerce. They are, however, short on personnel and the Coast Guard cutter fleet is older than 39 of the world's 41 major naval fleets.[91] Administration plans to upgrade ships and air patrol will not be complete until 2022.[92]

We should turn the Coast Guard into a 21st century force by increasing its manpower and firepower to match its mission. Congress should increase the Coast Guard's strength by 15 percent to turn it into a maritime force that is 50,000 strong. We should also accelerate the upgrading of frontline ships and planes (Project Deepwater) so that the new force is ready in the next ten years rather than the current pace of twenty years.

Check Cargo for Weapons of Mass Destruction

Millions of cargo containers enter the United States and travel through our communities every year. Currently, less than 5 percent of the cargo containers entering American ports are physically inspected to determine their contents. This Administration has not deployed the personnel or equipment necessary to ensure that these containers are free of weapons of mass destruction.[93]

Technology should be deployed to each sea and land port of entry to enable 100 percent of all cargo containers entering the United States to be screened for nuclear and radiological materials without engaging in cumbersome physical inspections that will slow commerce.

Implement Port Security Plans

Prior to September 11, the security at many American seaports ranged from poor to fair.[94] Many ports are developing plans to provide the security necessary in the post-September 11th world, such as installing cameras, building fences, and posting guards. Yet, the Administration has provided virtually no support for these efforts in its post-September 11 budgets. Due to the lack of funding and commitment, many ports are struggling to get these changes in place, leaving them extremely vulnerable.

Ports must receive the resources they need to improve their security.

Improve Aviation Security

Protect Passenger Planes from Missile Attack

Passenger planes are totally undefended against attack by surface to air missiles. Tens of thousands of these missiles are scattered across the globe and readily available for purchase on the black market. They are of known interest to terrorists and have been used against civilian aircraft in Kenya and most recently Baghdad.[95] Technology is being developed to help defend vulnerable civilian aircraft from surface to air missile attack.

The Department of Homeland Security must accelerate research for on board anti-missile technology for passenger aircraft, improve perimeter security, and deploy missile defenses as warranted by the threat as soon as technically feasible. Additionally, the Administration should pursue international programs to counter the proliferation of these missile systems and train border inspectors to prevent their entry into the United States.

Screen All Cargo on Passenger Planes

Today, 22 percent of all air cargo moves on passenger flights without a security check, despite a law that says the Transportation Security Administration (TSA) will screen all cargo.[96]

TSA instead relies on "known shippers" despite evidence of numerous security violations.[97] Screening passengers without screening the cargo carried beneath their feet invites disaster.

The Department of Homeland Security should establish a physical screening process for all cargo placed on passenger planes.

Screen All Baggage on Passenger Planes

Despite multiple requirements and missed deadlines, the (TSA) is still not electronically screening 100 percent of checked baggage. In some cases, TSA only ensures that a passenger is on board before a bag is loaded, a policy providing no security from suicide attacks.

The Department of Homeland should comply with the legal mandate for 100 percent electronic screening of baggage.

PROVIDING SECURITY INSIDE AMERICA

Terrorists have made it clear that attacking critical infrastructures achieves their dual aims of taking American lives and disrupting our economy.[98] For example, there are over 7,000 U.S. chemical facilities where a toxic release could kill or injure over 10,000 people; an accident at any one of over 120 of those facilities could threaten over 1 million people. As the deadly Madrid train bombing demonstrated, rail and other public transit are extremely vulnerable to attack. The millions of rail and truck cars carrying toxic and combustible chemicals around the country daily are potential bombs on wheels. Intelligence officials have warned against threats to water supplies, dams, and airplane attacks against nuclear facilities. Every day, millions of citizens are potential targets at concentrated travel points like bridges, tunnels, and subway stations and at concentrated settings like large buildings and public entertainment venues. We often make the mistake of defending against only the most recent attack. But it is likely that next time the terrorist will exploit a far different vulnerability than they did on September 11. We must harden as many of our infrastructures as possible to try and prevent, or at least mitigate the damage from, the next terrorist attack.

Passenger Rail and Transit Security

Worldwide, roughly one-third of terrorist attacks target transportation systems; the most frequently targeted transportation mode is public transit.[99] The attacks in Madrid are the most recent example of 195 terrorist attacks from 1997-2000.[100] Although terrorist attacks similar to the Madrid attacks or the frequent bus bombings in Israel have yet to occur in the United States, the threat is real and hard to protect against.

Some ten million train and subway trips are taken every day in the U.S., of which 66,000 travel on Amtrak on the one of the busiest corridors in the world, between Washington and Boston. Five times as many Americans travel on trains and transit each day then those that travel on planes.[101] Yet, the resources dedicated to rail and transit security are woefully inadequate.

Invest In Security Measures

DHS's 2004 fiscal year budget has $4.3 billion for aviation security, but less than 2 percent of this amount - $85 million – for ground transportation security, which includes not only trucking, but also rail and mass transit.[102] In the fiscal year 2005 budget request, spending on maritime and land transportation fell below three percent of TSA's budget.[103]

The cost in terms of security is real. According to a GAO survey and interviews with transit officials nationwide, "insufficient funding is the most significant challenge in making their transit systems as safe and secure as possible." In fact, survey respondents were more than 2.5 times more likely to cite insufficient funding as the main impediment to security relative to any other factors.[104]

The total estimated cost of security improvements at eight large transit agencies totaled $711 million. Extrapolating this estimate suggests that providing a baseline of security to the 50 largest metropolitan areas would cost roughly $2 billion.

The Administration should increase grant funding for passenger rail and transit by fivefold to $250 million in fiscal year 2004 to provide a down payment on enhancing security for passenger rail and transit throughout the United States.

Clarify Responsibilities on Rail/ Transit Security

According to the GAO, "The roles and responsibilities of TSA and [the Department of Transportation] in transportation security have yet to be clearly delineated, which creates the potential for duplicating and/or conflicting efforts as both entities move forward with their security efforts…DOT and TSA have not yet formally defined their roles and responsibilities in securing all modes of transportation."[105] In 2003, GAO recommended that the DHS Secretary work with the Secretary of Transportation to "develop a risk-based plan that specifically addresses the security of the nation's rail infrastructure" and "establish time frames for implementing specific security actions."[106] The GAO and DOT disagreed with the recommendation, and clear definition of roles and responsibilities remains absent.

DHS should develop a national transportation security strategy to help stakeholders set priorities, leverage resources, establish performance expectations, and create incentives for stakeholder to improve security.

The DHS Secretary should work with Secretary of Transportation to develop a risk-based plan that specifically addresses the security of the nation's rail and transit infrastructure and establish time frames for implementing specific security actions.

Chemical Facility Security

The Environmental Protection Agency (EPA) has identified 123 facilities in the U.S. that could threaten over one million people in the event of a massive breach of chemical containment, and over 7,000 U.S. chemical facilities where a toxic release could kill or injure over 10,000 people.[107] A 2002 Brookings Institution report ranks an attack on a chemical facility behind only biological and nuclear attacks in terms of possible fatalities.[108]

While chemical facilities and materials are essential components of our economy, they are also attractive targets to terrorists: capable of causing large loss of life and poorly defended. As recently as this holiday season, DHS officials warned of possible targeting of chemical plants by terrorists.[109] The Justice Department has described the threat to chemical plants as "both real and credible" and potentially more dangerous than an attack on a nuclear power plant.[110]

Recent reports suggest that the security surrounding industrial chemicals is weak. In November 2003, the television magazine *60 Minutes* reported unlocked gates, absent guards, dilapidated fences, and unprotected tanks filled with deadly chemicals at dozens of facilities in several major metropolitan areas.[111] In the Pittsburgh area, one reporter found easy access to over 200 tons of corrosive chlorine gas at four different sites.[112]

The seriousness and immediacy of the threat to our chemical infrastructure requires immediate steps:

Require Chemical Facilities to Assess and Address Security Vulnerabilities

Following September 11, many chemical facilities took voluntary actions to improve security. While laudable, these efforts have not been sufficient. Not all companies have taken voluntary steps, and there is little oversight for those that have. According to the General Accounting Office, "no federal oversight or third-party verification ensures that voluntary industry assessments are adequate and that necessary corrective actions are taken."[113] As a result, the extent of security preparedness at U.S. chemical facilities is unknown, and facility operators, law enforcement, and emergency responders may not be prepared to respond appropriately to security threats.

The Administration itself has advocated action. Over a year ago, DHS Secretary Tom Ridge and former EPA Administrator Whitman publicly stated that "voluntary efforts alone are not sufficient to provide the level of assurance Americans deserve" and chemical facilities "must be required to take steps" to improve security.[114] In the 30 months since September 11, however, the Administration has taken only "preliminary steps" towards ensuring the security of these vulnerable facilities.[115] DHS officials have visited only 17 plants and must rely wholly on industry supplied information and voluntary action.[116]

> *Congress should require all facilities that may pose a substantial danger to conduct vulnerability assessments, develop security plans to address vulnerabilities, and implement them. Federal standards setting, oversight, inspection, and strong enforcement authority by DHS and EPA would ensure compliance. Vulnerability assessments and security plans should be reviewed by government officials to ensure compliance and provide oversight. The pooling and sharing of information about security practices will assist government, industry, and first responders in constantly improving security and emergency response strategies.*

Improve Security by Promoting Inherently Safer Technologies

According to President Bush's science advisor, Dr. John Marburger, technologies that reduce the toxicity, flammability, or other hazardous characteristics of chemicals and their processes "help improve the environment, public health, and competitiveness," and also "inherently reduce the threat of terrorism."[117] Replacing dangerous chemical products and processes with "inherently safer technologies" (IST) will fundamentally reduce and possibly eliminate the danger posed by a chemical facility. Taking these steps is the only way to remove these targets from terrorists' lists.[118] But the Administration has opposed legislation requiring facilities to consider adopting IST where practicable[119] and has systematically undermined the chemical security activities of the only federal agency with expertise in IST, the EPA.[120]

> *Chemical producers and users should be required to consider using IST or other "alternative approaches" that can make a chemical or chemical process less hazardous. Information regarding the economic and technological barriers to its adoption to improve security should be collected and, with the leadership of EPA, an analysis undertaken that will identify opportunities across the industry where IST can improve security and suggest areas for research that will enhance IST and its adoption in the future.*

Agro-Terrorism And Food Safety

A strong, vibrant agricultural sector is an essential part of the U.S. economy, making up 13% of our GDP, and our safe, secure food supply is enjoyed by every single American. However, these crucial assets are highly vulnerable to willful and targeted disruption.

Past, unintentional introductions of pathogens demonstrate the danger. The discovery of a single case of mad cow disease in the U.S. has seriously damaged international trade in U.S. beef. In 2001, an outbreak of foot and mouth disease in the United Kingdom, caused by a highly contagious and easily introduced virus, cost that country over $10 billion in economic losses.[121] The Department of Agriculture conducted a simulation of an intentional release of this same virus in the U.S. and found that a single truckload of contaminated hogs could spread disease to 25 states within five days before detection.[122]

Unintentional food-borne illnesses remain a serious health threat, sending over 300,000 people to the hospital each year.[123] The recent outbreak of hepatitis A that harmed consumers of a shipment of Mexican green onions has demonstrated to observing terrorists the ease with this method of reaching a widespread range of victims with little risk of capture.[124] The terror alone from a real or suspected contamination of the food supply could be substantial. In 1989, Chilean grapes were widely rumored to be laced with cyanide poison. Although no evidence was found, public fears cost at least $210 million in damages.[125]

Terrorists have recognized these vulnerabilities. In a 1984 incident in Oregon, domestic bioterrorists sickened 750 people by contaminating a restaurant salad bar with salmonella bacteria.[126] In Afghanistan, U.S. agricultural documents and training manuals that included extensive sections on agricultural terrorism were discovered in al-Qaeda safe houses.[127]

These threats to our agricultural base and food supply must be addressed.

Strengthen Border and Facility Inspections

Defense against agricultural terrorism begins at the border, where the introduction of pathogens and contaminants can be stopped. But inspection at U.S. borders remains weak, with the FDA inspecting only 2 percent of food imports under its jurisdiction. Meanwhile, serious concerns exist about the adequacy of DHS inspectors' training and workforce.[128] DHS has not filled all available agriculture specialist positions[129] and between 50 to 75 percent of the current staff may transfer to alternative positions when permitted.[130] This will create a gap in our ability to inspect agriculture shipments coming across our borders.

Within the U.S., the highly integrated nature of our food distribution system means numerous access points for the terrorist as food travels from "farm-to-fork," moving thousands of miles and changing hands repeatedly.[131] The flow of livestock and crop shipments is often not traced.[132] At thousands of food processing and packing plants across the country, basic security is poor, personnel are rarely screened, and inaccurate or nonexistent recordkeeping practices make tracing contaminated food complicated and time-consuming.[133] While federal agencies have issued security guidelines and new registration requirements, they lack the authority or the manpower to enforce their adoption.[134]

> *Well-trained inspectors at airports, seaports, and land crossings are essential, and DHS should seek full and stable staffing of these positions. The inspection workforce of the USDA and FDA needs to be boosted to increase inspections to*

ensure compliance, but these resources cannot be increased indefinitely. The federal government should develop a program to train state and local inspectors to recognize exotic animal and crop diseases, the signs of terrorism, and understand biosecurity best practices. The job of all inspectors will be made much easier with rapid, sensitive diagnostic techniques for pathogens. The development of such devices and techniques must be a priority. A nationwide electronic livestock identification system should be deployed that is capable of tracing, within 48 hours, an individual animal from birth to slaughter.

Enhance Detection of Agro-Terrorism

The ability to rapidly detect an outbreak is vital to minimizing harm to people and the economy and reducing terror. But disease surveillance is hampered by farmers reluctant to report disease, underdeveloped communication channels between officials, poorly trained veterinarians, and inadequate diagnostic tools and laboratory capacity.[135] As a result, an outbreak of certain diseases might go unnoticed for long periods. In other instances, widespread outbreaks would quickly overwhelm laboratories or lead to misjudgments about the true extent of the spread of disease.

Surveillance is the most important tool for detecting contamination of the food supply. CDC's only active surveillance program for food-borne illnesses, FoodNet, covers less than 15% of the U.S. population.[136] In addition, the microbial monitoring of food, done at processing plants and ports of entry, is fragmented and is not sufficiently integrated with surveillance to detect pathogens in the food system.[137]

Active surveillance of food-borne illnesses, particularly those caused by pathogens likely to be intentionally introduced, must be expanded more quickly. Ultimately, a nationwide program should be employed. Rapid, clinical diagnostic tools for major food supply threat agents should be developed and supplied to practitioners. Results from food sampling and inspection data need to be further integrated into food-borne surveillance systems. This effort, combined with targeted research, will enhance already widely practiced safety assurance methods to detect intentional food contamination.

Prepare a National Agro-terror Response Plan

Preparedness for agricultural terrorism is also weak. The current food safety system remains a patchwork of up to 200 different agencies functioning under different regulatory approaches, operating in an uncoordinated fashion.[138] There is no comprehensive plan or strategy to prepare and defend the nation against terrorist attacks on our agriculture and food supply[139] and numerous gaps remain in our ability to rapidly and effectively respond.[140]

The Department of Homeland Security should lead in developing a comprehensive national strategy to prevent and respond to acts of terrorism against the nation's food supply and thwart the entry of harmful agents into the U.S. that would threaten our agricultural sector. Plans must include a strategic stockpile of animal vaccines, antibiotics, and insecticides, as well a rapid-reaction reserve of veterinary and plant pathologists who can respond to combat a serious outbreak. The sequencing of likely pathogen genomes should take on a high priority

and these data should be applied to a vigorous program in animal vaccine and drug development and genetically resistant crop science.

Cybersecurity & Information Warfare

According to a survey conducted last year by the Pew Internet and American Life Project, almost half of Americans fear terrorists will launch cyberattacks on our critical infrastructures, disrupting major services and crippling economic activity.[141] This fear is not unwarranted. Our power systems, telecommunications networks, financial sector, emergency, and national defense services all depend on computer networks – networks that are interconnected and reliant upon one another.

Our nation is only as strong as the security on the weakest link on these networks. A weak link on any computer can allow a hacker to open a dam, close down an air traffic control system, or create financial ruin for our banking industry. It was only a few years ago that a computer hacker gained control of a telephone system and disabled the Worchester, Massachusetts airport, shutting down the airport for more than six hours.[142] Others have penetrated the computer systems of the California Independent System Operator, the nonprofit corporation that controls the distribution of 75 percent of the state's power, and the Roosevelt Dam in Arizona.[143] In 2000, someone gained access to a utility company computer in Australia, releasing millions of gallons of raw sewage into a community's waterways.[144] In 2003, the Sobig computer virus temporarily shut down the 23,000-mile-long CSX rail system.[145]

These are only a few examples of the physical havoc that can be caused by cyberterrorists. The potential economic damage to our economy is also devastating and could be in the hundreds of billions of dollars. During the summer of 2003, three viruses, Sobig, Blaster, and Welchia, caused more than $32.8 billion in economic damages.[146]

We know that terrorists, as well as their supporters, are technologically-savvy. Soon after September 11th, hacker gangs such as "GForce Pakistan" declared a "cyber jihad" on the United States and called on all Muslim hackers to participate.[147] In October 2001, GForce defaced a government website posting a message stating, "Osama Bin Laden is a holy fighter…whatever he says makes sense." It also said that it planned to hit major U.S. military and British web sites and proclaimed an "Al-Qaeda Alliance online."

According to the Institute for Security Technology Studies at Dartmouth College, "terrorists are known to be extensively using information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely."[148] In addition to terrorist groups, several nation-states are known to be involved in developing cyberweapons.[149] Among those nations developing cyberwarfare capabilities are North Korea, Cuba, China, and Russia.[150]

Unfortunately, terrorists will only continue to expand on their technology capabilities. According to Dorothy Denning, author of one of the first books on cybersecurity and information warfare, our country must realize that "the next generation of terrorists will grow up in a digital world." Their skill and experience will be greater than today's terrorists. Indeed, cyberterrorism "could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet."

Securing our networks must be a priority in the war against terror. We cannot wait for a disaster to happen before we devote our full energies to preparing for and being able to respond to this threat.

Create Cybersecurity Crisis Center

If an electronic 9-11 were to happen tomorrow, who in the government could coordinate the efforts of dozens of agencies and effectively reach out to the private sector, which owns 85 percent of our critical infrastructures? It is not clear who has the authority and capability within the federal government to bring together the various federal and state agencies, as well as the relevant private sector entities, in the event of a cyber-catastrophe.

> *The challenges of protecting our critical networks and infrastructures require a new paradigm of government and industry leadership for addressing a crisis as it emerges. What is needed is a National Crisis Coordination Center that could house within a single physical facility critical infrastructure sector representatives, and federal, state, and local government agencies. This center would be multi-agency and include all agencies tasked with responsibilities relating to responding to attacks on our critical networks. At the same time, the center would house private sector representatives so that those who own and operate 85% of the infrastructures would be available in the event of a cyber "9-11." Such a center could bring together the best of the federal government and private sector.*

Make Cybersecurity A Priority

In February 2003, the Administration released a "National Strategy to Secure Cyberspace," setting forth five cybersecurity priority areas, including the development of a cybersecurity response system, a threat and vulnerability reduction program, and awareness and training programs, as well as plans for securing government computers and developing national security and international cooperation. Implementation of the plan has been delayed for over a year and three presidential advisors on cybersecurity have left the government, one after only two months. Indeed, the latest individual responsible for reporting to the President on critical infrastructure protection, including cybersecurity, left the White House's Homeland Security Council in February and has yet to be replaced.

> *We cannot continue to wait to protect our computer networks. We should move forward to meet the challenges presented by modern technology and eliminate the weakest links in our networks. We should develop a culture of security within our computer networks and among our citizens to ensure our national security. We need leadership within the government to assure that the United States is ready for attacks on our computer systems, especially in a time of crisis. If we do not take action, we leave our nation at risk.*

Prepare for Information Warfare

Information warfare "consists of those actions intended to protect, exploit, corrupt, deny, or destroy information resources in order to achieve a significant advantage, objective, or victory over an adversary."[151] For example, during the Gulf War, it was reported that a group of Dutch hackers indicated to Saddam Hussein that they would disrupt the U.S. military's deployment to

the Gulf for $1 million. Fortunately, Saddam declined the offer. Infowarfare can also try to disrupt or damage what we think or know about the world and about our country. Infowarriors use propaganda, media interference, computer hacking, and other efforts to promote "dissident or opposition movements across computer networks."[152]

The emergence of technology has made information warfare a viable threat. Not only must the United States protect its infrastructures, it must assure the availability and integrity of the information contained on them.

Critical Infrastructure

Besides protective measures specific to individual sectors, the government needs to develop a comprehensive approach to infrastructure protection that increases security and hardens targets across all sectors. The following steps need to be taken to begin the difficult process of identifying and addressing the many vulnerabilities in U.S. critical infrastructure:

Complete National Critical Infrastructure Risk Assessment in One Year

According to the Homeland Security Act, the DHS is required to comprehensively assess critical infrastructure vulnerabilities, prioritize protective measures, and develop a comprehensive national plan for securing critical infrastructures. Although the need for a national critical infrastructure risk assessment to prioritize protective efforts is widely accepted,[153] little has been done to perform the assessments. According to James Gilmore, Chairman of the Gilmore Commission, none of the Administration's various homeland security strategies were based on an adequate risk assessment,[154] the lack of which "hampers defensive measures and preparedness activities."[155]

In September, 2003, DHS' Assistant Secretary for Infrastructure Protection Robert Liscouski testified to the House Select Committee on Homeland Security[156] that he "would be surprised, frankly, if we had [a comprehensive risk assessment] done in the next five years." Five years is too long to wait when the threats exist now.

The DHS should, in coordination with other public and private partners, assemble within one year an initial/draft national critical-infrastructure risk assessment. Such an assessment should include a full assessment of threats, vulnerabilities, and consequences, and leverage, to the fullest extent possible, already existing risk assessments that have been performed by many states, infrastructure sectors, and federal agencies. The study should be updated and improved on an annual basis. In addition, the Congress should establish an Independent Commission to assess critical-infrastructure security and suggest strategies for the protection of the nation's critical infrastructures.[157]

Provide Incentives to Promote Investments in Infrastructure Security

The Administration has failed to provide leadership to improve critical-infrastructure security, 85 percent of which is owned by the private sector. According to the Brookings Institution, the Bush Administration "largely ignores" major critical infrastructure in the private sector.[158] In testimony before the House Select Committee on Homeland Security, homeland security experts gave the DHS "not a passing grade" on critical infrastructure protection.[159] The extent of the

Bush Administration policy to date is a nearly singular reliance on voluntary private action. Unfortunately, "private markets by themselves do not provide adequate incentives to invest in homeland security."[160]

> *The Administration should promote smart investments in critical infrastructures to improve both security and overall reliability, making critical infrastructures less vulnerable to potential disruption, whether terrorism-related or not. The Administration should use all the policy tools at its disposal to change the structure of incentives to increase the security of critical infrastructure in the United States, including tax incentives, promotion of terrorism insurance and other commercial products, and work with owners of critical infrastructure, as necessary, to ensure a minimum regulatory framework that helps promote security in each of the critical infrastructure sectors without placing unreasonable burdens on business owners.*[161]

Improve Information Sharing between Government and Owners of Critical Infrastructure

The Administration has made little progress on achieving effective information sharing between all levels of government and private owners of critical infrastructure protection. Information sharing is largely *ad hoc* and the Administration needs to make these relationships more explicit, more trusted, and more institutionalized. According to the GAO,[162] the Gilmore Commission,[163] and the Partnership for Critical Infrastructure Security,[164] the Administration has done little to delineate the functions, relationships, and mechanisms for information sharing in coordination with the critical sectors. Among problems cited by the GAO,[165] "none of the [levels] of government perceived the current information sharing process with the federal government to be effective… and the information that was shared was not perceived as timely, accurate, or relevant." Finally, the Markle Foundation has concluded the Administration has not taken advantage of America's technology expertise to enhance information sharing to combat terrorism.[166]

> *The DHS must dramatically improve information sharing by clearly defining roles and responsibilities, improving outreach and coordination, building robust institutions, better leveraging available technology, and strengthening accountability.*

Develop a Comprehensive National CIP Protection Plan

> *This plan would facilitate critical-infrastructure-protection information sharing that clearly defines roles and responsibilities of the Department of Homeland Security, other federal agencies, state and local governments, and private owners of critical infrastructure before, during, and after an attack on critical infrastructures. Establish comprehensive procedures for information sharing.*[167]

Create Metrics for Measuring Progress in Infrastructure Protection

The Administration should follow the recommendation of the Gilmore Commission that DHS "develop metrics for describing infrastructure security in meaningful terms, and to determine the adequacy of preparedness." The DHS should prepare an annual report card which assesses the state of preparedness of each of the critical infrastructure sectors against specific performance metrics. In addition, DHS should grant annual awards recognizing significant improvements or achievements in critical-infrastructure protection. Such programs can be a powerful tool for government to motivate private sector actors to enhance infrastructure security, as the public-relations impact of such assessments can be significant.

RESPONDING TO TERRORIST ATTACKS

According to a prominent bipartisan commission, America is "dangerously unprepared" to respond to a catastrophic terrorist attack. The September 11 attacks were a wake-up call to the nation that we must prepare, plan and be able to quickly mobilize to respond to any terrorist attack on our soil. Preparing America to meet this challenge means arming our first responders with the tools they need to respond to any situation and save lives, mobilizing second responders to strengthen preparedness and support first responders, and preparing the National Guard to assume a leading role in case of catastrophic attack.

Arm First Responders with the Tools They Need

Over two years after September 11th, there has been no systematic review of the true planning, equipment, training, and personnel needs of America's first responders in order to protect our communities from terrorist attacks. Although funding for some programs has increased, we have not defined the goals and objectives of this spending; we have not advanced the implementation of interoperable communications systems; nor have we identified the priority threats and vulnerabilities that limited homeland security funds should address.[168] [169] [170]

Determine the preparedness needs of our communities—including equipment, personnel, training, planning, and exercises—for firefighting, law enforcement, emergency medical services, public health, medical capabilities, and emergency management, that are flexible enough to be utilized for a wide range of threats and vulnerabilities. Create a Terrorism Preparedness Grant Program that will fund these needs, and get needed equipment and training in the hands of the police, firefighters and emergency personnel who will be the first on the scene of an attack.

Enable First Responders to Communicate

America's first responders still cannot talk with one another at a disaster scene. Communications equipment still is not interoperable and that means that too often at a disaster site, firefighters, police, and emergency personnel cannot communicate. There are at least six Federal departments and a number of interagency and independent organizations that are involved in developing standards for communication systems and equipment. Over two years after September 11, and over eight years after a federal advisory committee stated that immediate measures needed to be taken to promote interoperability, the situation remains as disconnected as ever.[171] [172] The technology exists today to overcome these barriers.

Enhance interoperable communications and allow first responders to take effective and coordinated action by deploying nationwide more cost-effective and efficient solutions to achieve radio system interoperability in the near future, utilizing available solutions that take advantage of the existing communications infrastructures within our states and localities. Centralize the administration of interoperable communications research, standards development, and grant management within DHS.

Expand Urban Search and Rescue Teams

The National Urban Search and Rescue (US&R) Response System is managed by Federal Emergency Management Agency to provide a highly-specialized and technical response capability in order to rescue victims of structural collapse to save lives, treat injuries and minimize secondary damage to structures. Each of the 28 current US&R Task Forces draws upon a base of local expertise, and has up to hundreds of members on-call for deployment in order to provide built-in redundancy for each Task Force. Last year, the Department of Homeland Security provided assistance to train and equip all 28 of the US&R Task Forces to address a situation involving weapons of mass destruction. Previously, only six (6) Task Forces were fully prepared to respond to WMD incidents.[173]

The Department of Homeland Security should set a response standard that mandates the ability to provide US&R Task Force assistance to every community in the nation within six hours of a terrorist incident or natural disaster.

Deploy Defenses for a Chemical Attack

The history of use of chemical weapons by terrorists proves that we must be prepared. We must not send our first responders into the chemical equivalent of the World Trade Towers.

Firefighters, police officers, and EMTs must be equipped with appropriate and effective protective gear to respond to a contaminated area. Where effective antidotes exist, every ambulance crew in the nation should be equipped with the supplies and training to treat victims at the scene. When new tools are needed, the development and licensing of antidotes for potential chemical agents and toxins should be vigorously pursued.

Support Second Responders

Since September 11, many Americans have been searching for a way to join the fight against terrorism. The federal government should facilitate and work in coordination with the private sector and small businesses to actively involve citizens in preparedness efforts. Public-private partnerships, such as the partnership between the Business Executives for National Security and the State of New Jersey and Georgia, have proven to be useful in identifying and coordinating private sector support for state and local first responders.

The Department of Homeland Security should support the development of "Second Responder" initiatives in all fifty states.

Strengthen National Guard Capabilities For Homeland Security

At present, the Army National Guard is primarily organized and equipped to conduct sustained combat overseas, with a very small percentage eventually dedicated to homeland security functions in the United States. Adjusting to the new strategic threats faced by the United States, the National Guard should devote more resources to provide greater support to civil authorities in preparing for and responding to homeland security responsibilities, and in particular, potential catastrophic terrorist attacks.[174] Homeland security should be made a top priority mission for a more significant portion of the National Guard. Geographically dispersed, with deep ties to local communities and well-established relationships with state governments, the National Guard is ideally suited—along with United States Northern Command—to be the military's primary contribution to homeland security. Aspects include:

Enhance National Guard's Homeland Security Mission

> *All Army and Air National Guard personnel should be trained and equipped with an enhanced focus on consequence management in the event of a major terrorist attack. The Guard should specifically prepare for assuming the lead military role in consequence management in case of a terrorist attack using nuclear, biological, chemical or radiological weapons in the United States. This will ensure that Guard personnel, who are not deployed overseas, will be able to respond in the event of a terrorist attack.*

Provide the United States with Regional National Guard WMD Response Units

The Department of Defense has received congressional approval to deploy Civil Support Teams (CST), specialized National Guard units that are trained to respond in the case of a WMD terrorist event against U.S. population centers in each state and several territories. Their function is primarily diagnostic in nature and they do not perform a consequence management role. They determine the nature of an attack, provide medical and technical advice, and provide guidance as to which follow-on response capabilities will be necessary. With additional training, they could play a more vital role in assisting local first responders such as firefighters and policemen in responding to attacks involving hazardous materials or weapons of mass destruction.

Currently, there are 32 full-time, 22-member teams. The fiscal year 2003 National Defense Authorization Act required a full-time WMD-CST in each state or territory, and the fiscal year 2004 Defense Appropriations Act provided funding for 12 additional CSTs. Rather than individual state teams, each with a small number of personnel having a limited function, these teams should be combined into larger regional teams whose members have greater initial response capability and can be deployed within a short period of time. The home-base of the regional teams would be based on an assessment of risk, desired response time, and the location of other WMD-response assets.

> *The United States should have eight to ten Rapid Response Regional Civil Support Teams capable of responding to a WMD terrorist attack within 4 hours. The teams should have both diagnostic expertise and the ability to support the efforts of first responders following a WMD incident.*

Conduct Annual Homeland Security Training and Exercises for Guard Units

Every National Guard unit should conduct annual full-scale exercises centering on its homeland security mission. The Guard units should coordinate their training, activities and planning with state and local first responders.

REINFORCING SECURITY, PRIVACY, AND CIVIL LIBERTIES

Scrutinize Emerging Technologies

The protection of our citizens' civil liberties and privacy is fundamental to the American way of life. Our security efforts are, after all, designed to preserve the "unalienable rights that are essential to the strength and security of our nation: life, liberty, and the pursuit of happiness."[175] At the same time, emerging technologies continue to become more sophisticated. In recent years, communications, surveillance, and database technologies, as well as biometrics and interconnected networks, have changed our terrorist-fighting capabilities. As we evaluate how to use these powerful tools, we must consider the implications for our "individual privacy and personal liberties."[176]

Benjamin Franklin said, "They that would give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." Our nation will lose the war against terrorist groups if they succeed in having us sacrifice our liberties at the altar of security. As Peter Swire and Jeffrey Eisenach, officials in the Clinton and Reagan Administrations, respectively, noted "We organize government not only to defeat terrorism and protect our nation, but also to maintain the heritage of freedom that gives those efforts meaning."

The federal government should convene a Privacy Commission to develop and issue clear, public guidelines governing the use of emerging technologies that have privacy and civil liberties implications. The Commission should also recommend rules to govern the collection, retention, and dissemination of information, including information provided by the private sector.

Review USA Patriot Act

To effectively fight the war on terror, our law enforcement and intelligence agencies must be equipped with the necessary legal authorities to find terrorists and prevent attacks. Six weeks after the September 11 attacks, Congress passed the USA Patriot Act. The Act increased the ability of law enforcement and intelligence agencies to more effectively share information about terrorists and their activities, broadened federal authority to track and intercept communications for both law enforcement and foreign intelligence gathering purposes, authorized the detention and deportation of alien terrorists, and added resources to fight terrorism financing.

Many parts of the USA Patriot Act provide important counterterrorism tools that have improved our capability to investigate and pursue terrorists. Concerns have been expressed, however, that some provisions of the legislation extend overly intrusive authorities to the government. Congress wisely provided that parts of the Act would expire in December 2005 so the efficacy of these provisions and their impact on personal liberty could be carefully assessed. Our country should have this important debate, as the Gilmore Commission put it, "in the quiet of the day," so that provisions of the law that make a positive contribution to the war on terror can be extended, and if necessary clarified and strengthened, while those that do not, or are overly broad, can modified or repealed.

A thorough review of the USA Patriot Act should be undertaken in the next session of Congress. Agencies should be required to explain how they use the powers granted to them and how these authorities contribute to the war on terror. Provisions that Congress determines have made a positive contribution to the government's counterterrorism efforts should be extended. Provisions that are rarely, if ever, used, and have had the effect of undermining public confidence in our law enforcement agencies, should be considered for repeal.